Declassified in Part - Sanitized Copy Approved for Release 2013/08/20 :
CIA-RDP91B00390R000200160010-0

Effective Steps Against Home-Grown Spies

By ANTHONY C. BEILENSON

When most of us think of espionage, we usually picture shadowy foreign agents who sneak into guarded facilities and steal vital national-security secrets. The reality, however, is quite another matter.

Virtually all of our most damaging and well-publicized espionage losses in recent years have been the result not of foreign agents who want to steal secrets but of U.S. citizens who want to sell them.

Today's spies come mostly from the lower ranks of our own military or intelligence agencies, and they are motivated by one of two things—money or revenge against their employers.

Yet, even though we have known for years that serious weaknesses in our ability to monitor these individuals are at the heart of our espionage crisis, we continue to depend on an outdated, ineffective personnel security system that has repeatedly failed to identify and catch spies before the damage is done.

Most of today's spies decide to betray their country after they enter government employment, not before. In other words, they do not enter the service of their country in order to steal its secrets; rather, they discover the value of those secrets once they have access to them, and are then unable to withstand the temptation to sell them to hostile intelligence services.

But we continue to focus our personnel security efforts almost entirely on pre-employment job screening, using extensive (and expensive) background investigations during the hiring process, even though we know that virtually no one seeks government employment intending to commit espionage. So it is not surprising that more than 98% of the applicants "screened" by this process receive a security clearance.

Meanwhile, many of the most vulnerable current and past employees—those who are the real targets of foreign intelligence services—do not even receive the routine five-year follow-up investigation required under current procedures.

Another important lesson that we have learned concerns not only whom we should monitor but also what we should look for in our security investigations. The discovery that spies are most often motivated by a desire for money suggests that one of the best places to look for the tell-tale signs of espionage is in the bank accounts of individuals who have access to highly sensitive information. Yet our personnel security investigations continue to ignore important and easily available financial data like credit records, large currency exchanges, foreign bank accounts, suspiciously large purchases or casino transactions. We have also ignored the warnings of spouses, girlfriends and family members, although in many cases they have been the first to raise suspicions concerning possible espionage.

Why, if these deficiencies are so well known, have we not yet corrected them? It's not that the needed reforms are prohibitively expensive. In fact, since most of the data on large financial transactions are already in the computer files of the Customs Service, we could make significant improvements, at virtually no cost, by simply cross-checking employees with security clearances against these computerized files. Similar corrective measures could also be made with little additional funding.

No, the greatest obstacle to correcting these deficiencies is not money. Rather, it is the mind-numbing size of the personnel security system itself. The federal government classified more than 22 million documents in 1985, adding these to a pile of a trillion others. To handle this mountain of secrets, we've issued security clearances to more than 4 million people.

We will never be able to adequately monitor this vast and still-growing bureaucracy. Some have suggested eliminating whole classification categories in order to stem the avalanche of new secret documents; others insist that a complete overhaul of the security system is the only way to genuinely protect our truly vital secrets. Everyone agrees, however, including the executive branch officials who preside over this system, that no plan to improve security can ever be adequate until the numbers of clearances and classified documents are drastically reduced.

In the meantime, we must learn to narrow the field of our investigations to those who handle the most sensitive information and are the most vulnerable to the temptations of espionage.

In case after case we have learned that real-life spies are most often motivated by prosaic, personal problems like financial distress, job disappointments and greed—issues that would not even make it into the first draft of a spy novel. Our adversaries have obviously known about and exploited these weaknesses for years. Now that we have learned this lesson, we must use it to fashion a more effective system for protecting sensitive information and catching spies.

Rep. Anthony C. Beilenson (D-Los Angeles) is the chairman of the subcommittee on oversight and evaluation of the House Intelligence Committee.